BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General
ANTHONY J. COPPOLINO
Deputy Branch Director
PAUL G. FREEBORNE
Virginia Bar No. 33024
Senior Trial Counsel
KIERAN G. GOSTIN
D.C. Bar No. 1019779
Trial Attorney

Civil Division, Federal Programs Branch
U.S. Department of Justice
P.O. Box 883
Washington, D.C. 20044
Telephone: (202) 353-0543
Facsimile: (202) 616-8460
E-mail: paul.freeborne@usdoj.gov

Attorneys for Federal Defendants

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

WILEY GILL; JAMES PRIGOFF; TARIQ RAZAK; KHALID IBRAHIM; and AARON CONKLIN,

Plaintiffs,

v.

DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

No. 3:14-cv-03120 (RS)

DFENDANTS' OPPOSITION TO PLAINTIFFS' SPECIAL MOTION TO ESTABLISH RIGHT TO DISCOVERY ON THE DEPARTMENT OF JUSTICE'S STANDARD FOR SUSPICIOUS ACTIVITY REPORTING

Hearing Date: August 20, 2015
Time: 1:30 p.m.
Judge: Hon. Richard Seeborg
Ctrm: 3, 17th Floor

Table of Contents

Table of Authorities

Cases

Statutes

Regulations

Other Authorities

INTRODUCTION

This case involves Plaintiffs' Administrative Procedure Act ("APA") challenge to the Nationwide Suspicious Activity Reporting Initiative ("NSI"), a program through which the federal government has encouraged federal, state, local, tribal and territorial ("FSLTT") partners to share reports of suspicious activity amongst themselves through one or more national databases. Compl., Dkt. 1 ¶ 2. Pursuant to his authority under the Intelligence Reform and Terrorism Prevention Act of 2004 ("IRTPA"), Pub. L. No. 108-458, 118 Stat. 3638 (2004), the Program Manager for the Information Sharing Environment ("PM-ISE") has issued several versions of a Functional Standard defining the type of "suspicious activity" information that should be shared in connection with the NSI. Defendants have filed an administrative record containing the non-privileged information that was considered in developing that definition. Dkt. 52, 53. Plaintiffs, however, also assert that the Department of Justice ("DOJ") has issued a distinct standard for suspicious activity reporting, Compl. ¶¶ 53–70, and have requested that the Court grant their motion establishing a right to conduct discovery on the existence and scope of that alleged standard. For a host of reasons, this discovery should not be permitted.

At the outset, it is helpful to explain that IRTPA is not the sole (or even the primary) statutory authority through which federal law enforcement receives information about suspicious activities, including reports of suspicious activities initially observed by state and local law enforcement. The FBI administers eGuardian—which is the primary Shared Deposit Repository ("SDR") through which FSLTT partners share information with one another in connection with the NSI. But the FBI is also authorized by other statutes and regulations to conduct investigative activities and collect information related to potential terrorism. Accordingly, regardless of whether FSLTT partners share information about suspicious activities with one another in connection with the NSI, the FBI still encourages them to report that information to the FBI even if it does not satisfy the definition of suspicious activity in Functional Standard.[1] This statutorily authorized information gathering is not part of the NSI and is not governed by IRTPA.

[1] FSLTT partners may use eGuardian (as well as other avenues) to report information to the FBI. As the documents cited by Plaintiffs make clear, information that is "reported" (rather than "shared") in eGuardian is not placed in the SDR and is not available to other FSLTT partners.

Nonetheless, through their special motion for discovery, Plaintiffs have attempted to expand this case from a relatively constrained challenge to the NSI to a broad inquiry into the FBI's general information-receipt function. The Court should deny Plaintiffs' motion for a variety of reasons. In resolving Defendants' motion to dismiss, the Court reserved decision as to whether Defendants had adequately pled claims arising from the purported "DOJ Standard." Defendants renew their motion to dismiss those claims because Plaintiffs have still failed to identify the content of the purported standard that they are challenging or to plead facts demonstrating that the issuance of this unidentified standard would be reviewable under the APA. Moreover, even if this Court decides not to dismiss Plaintiffs' DOJ Standard claims, it should permit Defendants the opportunity to move for summary judgment on the basis of the administrative record as well as any additional declarations needed to establish that a grant of summary judgment is appropriate. Consistent with principles of judicial review of administrative action, Plaintiffs would then be entitled to oppose that motion on the ground that the record should be supplemented or additional discovery permitted.

As noted, Plaintiffs have failed to adequately plead the existence of a separate DOJ standard. In their Complaint, Plaintiffs allege that the FBI "set forth the following standard for suspicious acitivity reporting: 'observed behavior that *may be indicative* of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention.'" Compl. ¶ 54 (emphasis in original). Plaintiffs now concede that this purported standard was identical to the then-operative Functional Standard and have abandoned their assertion that the DOJ has issued a "may be indicative" standard for suspicious activity reporting. Any challenge to the "may be indicative" standard therefore simply proceeds from Version 1.0 of the Functional Standard. And Plaintiffs have not identified any other specific standard that they claim to be challenging in its place. Instead, Plaintiffs appear to be seeking unfettered discovery into the FBI's general investigative practices for receiving information from local law enforcement. Plaintiffs, however, cannot simply challenge the FBI's general authority to collect information, nor obtain discovery into those activities, by merely alleging that some unidentified "standard" exists and asserting that it is being challenged in this case. This failure to identify the standard

that they are challenging does not satisfy minimum pleading standards and warrants dismissal.

Moreover, apart from this failure to identify the "DOJ standard" they are challenging, Plaintiffs have not pled facts establishing that the issuance of this unidentified standard constitutes final agency action subject to APA review, let alone a legislative rule subject to notice-and-comment rulemaking. Plaintiffs allege that the purported "DOJ standard" was issued through the FBI's release of its Privacy Impact Assessment for the eGuardian Threat Tracking System ("privacy impact assessment"). Compl. ¶ 54. Privacy impact assessments, however, are not used to issue substantive rules subject to APA review. They are reports required by section 208 of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002), that describe how an agency is handling particular information to ensure compliance with *applicable* legal, regulatory, and policy requirements regarding privacy. In other words, the privacy impact assessment simply describes the information that is stored within eGuardian and analyzes whether the storage of that information poses any privacy risks. It does not impose any obligations (or rights). In addition, the privacy impact assessment expressly states that the information FSLTT partners share with one another in the SDR should satisfy the definition of suspicious activity articulated in the Functional Standard. On its face, therefore, the privacy impact assessment does not create any new standard for the sharing of information among FSLTT partners.

Finally, as noted, even if the Court does not dismiss Plaintiffs' claims arising from the purported DOJ standard, the default is not to permit discovery. Instead, the Court should permit Defendants to move for summary judgment on all of Plaintiffs' claims on the basis of the administrative record already filed by Defendants, as well as any additional declarations needed to establish that a grant of summary judgment is appropriate. Plaintiffs would then be entitled, if appropriate, to oppose that motion on the ground that the record should be supplemented or additional discovery permitted. This approach is the normal course in APA cases, where the baseline rule is that discovery is not permitted. And following this approach here would allow the Court to consider Plaintiffs' demand for discovery with a fuller exposition of the relevant issues, including whether a valid APA claim even exists, than this response permits.

BACKGROUND

I. Procedural Background

Plaintiffs allege that the DOJ and the PM-ISE have issued separate standards governing the collection, maintenance, and sharing of suspicious activity reports among state, local, and federal participants in the NSI. *See* Compl. ¶¶ 42–70. In ruling on Defendants' motion to dismiss, the Court found that Plaintiffs had pled sufficient facts to show the existence of a "binding legal norm" in the Functional Standard that would constitute final agency action reviewable under the APA, Dkt. 38 at 8, and permitted Plaintiffs' notice-and-comment claim with regard to that standard to also proceed past dismissal. *Id*. at 10-11. The Court, however, did not determine whether there is a separate DOJ SAR Standard or that Plaintiffs' claims related to that standard could separately proceed as a matter of law. *Id*. at 2.

Following a subsequent Case Management Conference on March 12, 2015, the Court adopted Defendants' proposal that the PM-ISE submit an administrative record reflecting the information that it relied upon in developing the Functional Standard. Dkt. 41.[2] Given the unresolved issue with respect to the purported existence of a DOJ standard, and the implications it has for Plaintiffs' request for discovery, Defendants additionally suggested at that conference that Plaintiffs identify and articulate why they are entitled to discovery about the "DOJ standard." The Court agreed and Plaintiffs subsequently filed a motion to establish their right to discovery on the purported "DOJ standard." To succeed on that motion, Plaintiffs must point to facts alleged in their Complaint plausibly alleging that there is a distinct "DOJ standard" for the collection, maintenance, and dissemination of SARs among state and local jurisdictions, that the issuance of this standard constitutes final agency action subject to APA review, and that the issuance of this standard constitutes a legislative rule subject to the notice-and-comment rulemaking procedures in the APA.

[2] Defendants have since filed that administrative record. Dkt. 51, 52.

II. The FBI's Privacy Impact Assessment for the eGuardian System

Plaintiffs primarily rely on the FBI's release of a privacy impact assessment for the eGuardian System ("privacy impact assessment"), to demonstrate that the DOJ has issued a purportedly binding standard governing the FSLTT partner's collection, maintenance, and sharing of suspicious activity reports, Dkt. 51-1, that is distinct from the definition of "suspicious activity" in the Functional Standard. Compl. ¶¶ 54, 64-66. As discussed in more detail below, an agency's release of a privacy impact assessment is governed by the E-Government Act of 2002 and cannot provide the basis for Plaintiffs' APA claims. Indeed, Plaintiffs have not cited, and Defendants are not aware of, any case where a privacy impact assessment was subjected to review under the APA.

A. The E-Government Act of 2002

The FBI's privacy impact assessment, as noted, was released pursuant to section 208 of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002), which requires federal agencies to create a privacy impact assessment when developing or procuring certain information technology systems defined in the E-Government Act or initiating a new collection of information. The assessment must address what information is to be collected under the system, why the information is being collected, the intended use of the information, with whom the information will be shared, how individuals can consent to the use of their information, how the information will be secured, and whether a system of records is being created under the Privacy Act. Pub. L. No. 107-347, § 208(b)(1)(B)(ii). As explained in the Office of Management and Budget ("OMB") Guidance implementing section 208 of the E-Government Act, a "privacy impact assessment," is, *inter alia*, "an analysis of how information is handled . . . to ensure handling conforms with applicable legal, regulatory, and policy requirements regarding privacy[.]" M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003), *available at* http: //www.whitehouse.gov/omb/memoranda_m03-22, Attachment A, II.A.f thereto ("OMB Guidance").

Unlike legislative rules subject to the rulemaking procedures of the APA, section 208 of the E-Government Act does not require that privacy impact assessments be promulgated pursuant to notice-and-comment rulemaking. Rather, section 208 requires that an agency: (1) conduct a privacy impact assessment; (2) ensure review of that privacy impact assessment by the Chief Information Officer, or equivalent; and (3) "if practicable," make the "privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means," Pub. L. No., 107-347, § 208(b)(1)(B)(iii), before "developing or procuring information technology that collects, maintains, or disseminates information that is an identifiable form," *id*. § 208(b)(1)(A)(i), or "initiating a new collection of information" that is an identifiable form, *id*. § 208(b)(1)(A)(ii).

B. The FBI's eGuardian Privacy Impact Assessment

The FBI's privacy impact assessment for eGuardian was initially published on November 25, 2008. *See* Compl., Ex. E. It has been subsequently amended twice, first on January 4, 2013, *see* Dkt. 51-1, at 2–13, and a second time on January 14, 2014, *id*. at 13–18.

As explained in the privacy impact assessment, the eGuardian system is a platform that allows for the collection, maintenance, and sharing of certain information. Dkt. 51-1, at 2.

> By providing a common platform to law enforcement for the reporting and sharing of . . . threats[,] the FBI [is] able to provide a universal reporting system for all law enforcement, while concurrently eliminating the jurisdictional and bureaucratic impediments to sharing information which results in degradation of our national security posture.

Id. The eGuardian system was designed "to ensure that privacy controls and security controls" were integrated into the system's development and functionality. *Id.* The eGuardian system therefore fulfills two of the purposes identified in the congressional findings of the E-Government Act: (1) it "improve[s] the ability of Government to achieve agency missions," Pub. L. No. 107-347, § 2(b)(4); and (2) it "provide[s] enhanced access to Government information and services in a manner consistent with laws regarding the protection of personal privacy, national security . . . and other relevant laws," *id*. § 2(b)(11).

Consistent with the requirements of section 208 of the E-Government Act, the privacy impact assessment explains the type of information that is collected in the eGuardian system:

> eGuardian collects terrorism and cyber threat information, suspicious activity reporting with a potential nexus to terrorism, and information that exhibits a potential nexus to criminal activity. . .

Id. at 16. eGuardian thus maintains a variety of information, not just reports relating to suspicious activity.

With respect to the collection, maintenance, and sharing of suspicious activity reports, the privacy impact assessment explains that "[t]he 'suspicious activity' definition utilized by the FBI is consistent with the definition utilized by the ISE in the ISE–SAR Functional Standard," and further states that the "FBI adheres to the current ISE Functional Standard." Dkt. 51-1, at 16. At the time of last revision of the privacy impact assessment in January 2014, the operative Functional Standard was version 1.5, issued on May 21, 2009. *See* Compl. ¶ 56. Consistent with the then-operative Functional Standard, the privacy impact assessment defines "suspicious activity" as "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity." Dkt. 51-1 at 16.

The Functional Standard was recently revised on February 23, 2015, in version 1.5.5. Dkt. 51-3, at 7. Version 1.5.5 slightly altered the definition of "suspicious activity." Specifically, it changed the definition from "observed behavior reasonably indicative of pre-operational planning *related* to terrorism or other criminal activity," Compl. ¶ 58, to "observed behavior reasonably indicative of pre-operational planning *associated* with terrorism or other criminal activity." Dkt. 51-3 at 5 (change in italics). Because, as noted, the privacy impact assessment clarifies that "the FBI adheres to the current ISE Functional Standard and observes the ISE-SAR criteria," Dkt. 51-1, at 16, this slightly revised definition of "suspicious activity" applies to the administration of eGuardian. Indeed, the privacy impact assessment notes that the PM-ISE is currently operating on Functional Standard 1.5 and that "[a]n update is currently under review and certification with the [PM-ISE]." *Id.* at 13 n.5.

The privacy impact assessment also recognizes that the Functional Standard follows "a behavior-focused approach[.]" *Id.* at 16. As such, information may not be entered into eGuardian "based solely on the ethnicity, race, or religion of an individual; solely on the exercise of any other rights guaranteed by the First Amendment; or solely based upon the lawful exercise of any other rights secured by the Constitution or laws of the United States." *Id.* This behavior-focused approach, too, is consistent with the approach in the Functional Standard. *See* Dkt. 51-3, at 11 (describing the Functional standard as incorporating a "behavior-focused approach to identifying suspicious activity requires that factors such as race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion").

But as Defendants have previously made clear, not all information in eGuardian exists in connection with the NSI or satisfies the definition of suspicious activity in the Functional Standard. When information is uploaded to eGuardian, it may *either* be shared with other FSLTT law enforcement partners *or* reported solely to the FBI. Dkt. 51-1, at 16. Information that is shared should meet the definition of suspicious activity in the Functional Standard, while information that is reported to the FBI does not need to satisfy that definition. This reflects the limited applicability of the Functional Standard to the sharing of information among FSLTT partners in connection with the NSI. Dkt. 51-3, at 17–18.

Shared information is "placed in the SDR, where it will be viewable and searchable by members of the FSLTT [law enforcement partners] that are provided access to the eGuardian system." Dkt. 51-1, at 16. Shared information must meet one of the following criteria:

1. It must be reasonably indicative of pre-operational planning related to terrorism or other criminal activity and have a potential nexus to terrorism or cyber criminal activity. In this context, pre-operational planning describes activities associated with a known or particular planned operation or with operations generally (*e.g.*, terrorist financing not necessarily tied to specific plots); or

2. It must exhibit reasonable suspicion that the subject of the information is involved in criminal activity and the information is relevant to criminal conduct or activity (as set forth in 28 C.F.R. Part 23).

Id. The "reasonably indicative" standard parallels the Functional Standard and the reasonable suspicion standard exceeds that standard. Dkt. 51-3, at 10. The "reasonable suspicion" standard, as the privacy impact assessment notes, is drawn from 28 C.F.R. Part 23. Dkt. 57-1 at 16.

The FBI, however, has broad authority to collect information from local law enforcement to carry out its investigative and counter-terrorism mission. Pursuant to the FBI's general investigative authority under 28 U.S.C. § 533 and its general authority to collect records under 28 U.S.C. § 534, *see* Dkt. 51-1, at 9, eGuardian also includes a broader category of "reported" information. Reported information is *not* placed in the SDR or viewable by other FSLTT law enforcement partners. Dkt. 51-1, at 16. It can only be viewed by the authoring agency, the appropriate fusion center, and the FBI. *Id.* "[T]he eGuardian workflow architecture is designed to restrict the ability to view submitted incidents to the author of the report, the reporter's supervisor, and the fusion center prior to being reviewed and approved for sharing." *Id*. at 17.

Importantly, information reported to the FBI does not have to satisfy any articulated standard. Indeed, one of the primary purposes of the report function is to allow the FBI to use holdings to which it has unique access to determine whether the reported information can be shared consistent with the definition of "suspicious activity" in the Functional Standard. *Id.* at 17-18.

The FBI's independent collection and investigative authority, moreover, is specifically recognized in the Functional Standard. *See* Dkt. 51-3, at 17–18 (recognizing that "ISE-SAR process does not supersede other information and intelligence gathering, collection, or sharing, including the authority to share information between and among Federal agencies and [state and local law enforcement] agencies where the information is related to homeland security, terrorism, or other Federal crimes."). The Functional Standard thus recognizes, for example, that "terrorism-related leads that do not meet the requirements of the ISE-SAR Functional Standard but may require investigative follow-up by the FBI . . . may be submitted electronically to the FBI." *Id*. n.17.

ARGUMENT

Plaintiffs' "DOJ Standard" claims are based on the assertion that the FBI has issued a distinct standard imposing a legal obligation on FSLTT law enforcement partners to collect, maintain, and share suspicious activity reports in accordance with the requirements of that standard. But Plaintiffs have not identified the content of that standard or pled facts showing that the issuance of this unidentified standard constitutes final agency action or a legislative rule. Indeed, nothing in the documents cited by Plaintiffs supports the existence of a separate, APA-reviewable "DOJ-standard" that is subject to challenge as a distinct agency action, let alone justifies discovery into its existence. What Plaintiffs appear to be demanding is the right to take discovery into how the FBI generally collects investigative information outside of the PM-ISE process, but this request for discovery is not moored to any valid APA claim in this case.

I. Discovery Standard in an APA Action

The Court should deny Plaintiffs' special motion seeking discovery on the purported DOJ Standard. Before discovery is permitted in an APA action, Plaintiffs must overcome two hurdles. First, like any other claim, Plaintiffs must plead facts stating a plausible claim. *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2006). Plaintiff may not rely on "labels and conclusions." *Id.* Moreover, the "tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to legal conclusions." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Accordingly, claims that rely on threadbare factual allegations that do not cross the line from possibility to plausibility are insufficient to "unlock the doors of discovery." *Iqbal*, 556 U.S. at 678.

Second, because judicial review in an APA action is limited to the administrative record, *Fla. Power & Light Co. v. Lorion*, 470 U.S. 729, 743–44 (1985), *Fence Creek Cattle Co. v. U.S. Forest Serv.*, 602 F.3d 1125, 1131 (9th Cir. 2010), Plaintiffs have the additional burden of demonstrating that they are entitled to discovery under one of the narrow exceptions to record review. *See Bark v. Northrop*, 2 F. Supp. 3d 1147, 1152 (D. Or. 2014) (holding that it is the burden of the party seeking discovery to establish that an exception to the general bar on discovery in APA cases applies); *McCrary v. Gutierrez*, 495 F. Supp. 2d 1038, 1041 (N.D. Cal.

2007) (Seeborg, J.) ("Because a court's review of an agency decision is limited to the administrative record, discovery is generally not permitted in APA cases."). And here, where agency action is challenged under the arbitrary and capricious standard of review, *de novo* review is not permitted. *Camp v. Pitts*, 411 U.S. 138, 142 (1973). Accordingly, if an administrative record does not exist, that does not permit the development of "some new record made initially in the reviewing court." *Id*. at 142. The appropriate next step is instead "to obtain from the agency . . . such additional explanation of the reasons for the agency decision as may prove necessary" upon remand. *Id*. at 143.

II. Plaintiffs Have Failed To Plead a Cognizable Claim that Unlocks the Doors of Discovery

Plaintiffs have failed to overcome this first hurdle and plead facts that could "unlock the doors of discovery" with respect to the purported DOJ Standard. First, as an initial matter, Plaintiffs have simply not identified the content of the alleged standard that they claim to be challenging. This failure alone warrants dismissal. Second, Plaintiffs assertion that the FBI's release of the privacy impact assessment constitutes a final agency action subject to APA review or a rulemaking subject to the APA's notice-and-comment procedures is a mere legal conclusion that should not be credited by the Court. There are simply no factual allegations sufficient to demonstrate that the FBI's privacy impact assessment, which it was required to issue under section 208 of the E-Government Act, imposes any legal obligation on other entities or supports the existence of a separate, reviewable "standard" that constitutes an agency action subject to APA review. Third, the other documents cited by the Plaintiffs fare no better in establishing the existence of a legally binding standard for the collection, maintenance, and sharing of information.

A. Plaintiffs Have Not Identified a DOJ Standard that Is Distinct from the Functional Standard

Plaintiffs' assertion that their claims are plausible because they have alleged that the DOJ has a distinct standard for "SAR reporting" that is broader than the Functional Standard, Pls. Mem. at 7–9 (citing Compl. ¶¶ 53, 55), is incorrect. Indeed, as Plaintiffs now admit, the purported DOJ standard that they reference in their Complaint is identical to then-operative

Functional Standard and does not reflect the issuance of a distinct standard. And Plaintiffs have not identified any other purported DOJ standard that they claim to be challenging instead.

In their Complaint, Plaintiffs clearly state the content of the purported standard that they are challenging. Specifically, they allege:

> DOJ, through its component the FBI, has set forth the following standard for suspicious activity reporting: "observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal or other illicit intention." FBI, Privacy Impact Assessment for the eGuardian Threat Tracking System at § 1.1 (emphasis added). This standard is set forth in the FBI's 2008 eGuardian Privacy Impact Assessment ("2008 eGuardian PIA"), which is attached as Appendix E to this Complaint.

Compl. ¶ 54. Though Plaintiffs allege that this standard is distinct from the Functional Standard, that simply is not the case. Even assuming the privacy impact assessment constitutes or identifies a discrete "standard" subject to review (which it does not), its definition is identical to the definition of suspicious activity in Functional Standard 1.0, which was the operative Functional Standard when the version of the privacy impact assessment cited by Plaintiffs was released. Indeed, Plaintiffs now concede this point in a footnote to their motion. Pls. Mem. at 9 n.12 ("As explained above, the 2008 eGuardian PIA utilizes a definition of suspicious activity that is identical to ISE Functional Standard 1.0."). By their own admission, therefore, Plaintiffs' challenge to a separate DOJ Standard for suspicious activity reporting proceeds from the Functional Standard that *contains the same standard.*

Despite conceding this point, Plaintiffs attempt to search for some other basis to justify discovery into the FBI's investigative practices. Primarily, they focus on another outdated version of the privacy impact assessment to assert that DOJ has adopted a standard for the sharing of suspicious activity information that is not consistent with the Functional Standard. Pls. Mem. at 14–16 (quoting since-amended language from the January 2013 privacy impact assessment). This proves nothing, however, and certainly does not justify discovery. The January 2014 update to the privacy impact assessment clarifies that information shared with other FSLTT law enforcement partners through eGuardian must meet one of the following criteria:

1. It must be reasonably indicative of pre-operational planning related to terrorism or other activity and have a potential nexus to terrorism or cyber criminal activity. In this context, pre-operational planning describes activities associated with a known or particular planned operation or with operations generally (*e.g.*, terrorist financing not necessarily tied to specific plots); or

2. It must exhibit reasonable suspicion that the subject of the information is involved in criminal activity and the information is relevant to criminal conduct or activity (as set forth in 28 C.F.R. Part 23).

Dkt. 51-1 at 15.

These criteria do not constitute or describe any distinct DOJ standard subject to APA review. The reasonably indicative standard is from the Functional Standard and the reasonably suspicious standard is from 28 C.F.R. Part 23. Indeed, the privacy impact assessment expressly states that with respect to the sharing of information by FSLTT law enforcement partners "the FBI adheres to the current ISE Functional Standard and observes the ISE-SAR criteria," Dkt. 51-1 at 16. Accordingly, the language of the privacy impact assessment itself makes clear that it does not create any different DOJ standard.

Instead of identifying a particular standard that they are challenging, Plaintiffs appear to be seeking general discovery into the FBI's investigative practices. As explained, pursuant to various legal authorities, the FBI does collect information that does not satisfy the definition of suspicious activity in the Functional Standard. But Plaintiffs have not pled a challenge to the FBI's general information-receipt function. And if they had, such claims would not survive judicial scrutiny for a variety of reasons—including that programmatic challenges to an agency's general implementation of its statutory authority are not permitted under the APA. *Lujan v. Nat'l Wildlife Fed.*, 497 U.S. 871, 890 (1990).

In sum, as Plaintiffs concede, the so-called "DOJ-standard" that Plaintiffs seek to challenge, and upon which they now demand discovery into FBI investigative practices, is based on an outdated privacy impact assessment containing a definition of suspicious activity that was identical to the then-operative version of the Functional Standard. And Plaintiffs have not articulated any other purported standard that they are challenging that would satisfy minimum pleading standards. While Plaintiffs assert that they are entitled to discovery the existence of

such a legally binding standard, Pls. Mem. at 8, it is "no answer to say that a claim just shy of a plausible entitlement to relief can, if groundless, be weeded out early in the discovery process." *Twombly*, 550 U.S. at 546. Plaintiffs have failed to identify the purported DOJ standard that they are challenging, and they should not be permitted to go on a fishing expedition in the hope that they will ultimately be able to identify the standard that they assert they are challenging.

B. The Privacy Impact Assessment Does Not Impose Legal Obligations

In addition to their failure to identify the content of the standard they are challenging, Plaintiffs have failed to plead facts that would establish that this unidentified standard has imposed a substantive obligation on FSLTT partners that is reviewable under the APA. To establish final agency action, a necessary element of any claim under the APA, Plaintiffs must plead facts showing that the FBI has issued a standard "by which rights or obligations have been determined or from which legal consequences will flow." *Bennett v. Spear*, 520 U.S. 154, 177-78 (1997) (quotation marks and citations omitted); *see also Mamigonian v. Biggs*, 710 F.3d 936, 942 (9th Cir. 2013). And for their notice-and-comment claim to proceed, Plaintiffs must also plead facts that would show that the purported standard "create[s] rights, impose[s] obligations, or effect[s] a change in existing law pursuant to authority delegated by Congress." *Hemp Indus. Ass'n v. DE*A, 333 F.3d 1082, 1087 (9th Cir. 2003). To meet these requirements, Plaintiffs primarily rely on the FBI's issuance of a privacy impact assessment for eGuardian, but privacy impact assessments (such as that for the FBI's eGuardian system) do not impose the type of substantive legal obligations reviewable under the APA.

Section 208 of the E-Government Act, as noted, requires federal agencies to address what information is to be collected in an information technology system such as eGuardian, why the information is being collected, the intended use of the information, with whom the information will be shared, how individuals can consent to the use of their information, how the information will be secured, and whether a system of records is being created under the Privacy Act. Pub. L. No. 107-347, § 208(b)(1)(B)(ii). As the OMB Guidance for Implementing the Privacy Provisions of the E-Government Act explain, a privacy impact assessment simply provides "an *analysis* of how information is handled . . . to ensure handling conforms with applicable legal,

regulatory, and policy requirements regarding privacy[.]" OMB Guidance, *available at* http: /www.whitehouse.gov/omb/ memoranda_m03-22, Attachment A, II.A.f thereto (emphasis added).

In other words, a privacy impact assessment is a privacy risk assessment required by the E-Government Act. It does not set forth rules that could be considered final agency action "by which rights or obligations have been determined, or from which legal consequences will flow." *Bennett*, 520 U.S. at 177–78 (quotation marks and citations omitted). Accordingly, Plaintiffs' claims regarding the purported DOJ standard cannot be permitted to continue to discovery because there is no jurisdiction to hear these claims. *See Rattlesnake Coal v. EPA*, 509 F.3d 1095, 1104 (9th Cir. 2007) ("Absent final agency action, there was no jurisdiction in the district court to review the . . . claim); *Ukiah Valley Med. Ctr. v. FTC*, 911 F.2d 261, 266 (9th Cir. 1990) (finality is "a jurisdictional requirement" under section 704 of the APA).

Moreover, the Court's ruling that Plaintiffs have pled a sufficient cause of action to permit their claims with respect to the Functional Standard to proceed, Dkt. 38, at 9, does not establish the existence of final agency action with regard to the purported DOJ standard. While the Court found that the Functional Standard required NSI participants to submit SARs consistent with the Functional Standard, that ruling does not apply to the purported DOJ standard or the privacy impact assessment. Nothing in the text or structure of the E-Government Act or the privacy impact assessment itself demands compliance by FSLTT law enforcement partners. Indeed, as explained, Plaintiffs have not even identified the content of the alleged DOJ standard that they assert has been imposed on FSLTT partners.

To be final agency action, the privacy impact assessment must have "'the 'status of law'" and demand "'immediate compliance'" by NSI participants. *FTC v. Standard Oil Co. of Cal.*, 449 U.S. 232, 239 (1980) (quoting *Abbott Labs. v. Gardner*, 387 U.S. 136, 153 (1967)). But the privacy impact assessment neither "commands" NSI participants "to do or forbear from anything." *Fairbanks v. North Star Borough v. U.S. Army Corp. of Eng'rs.*, 543 F.3d 586, 592 (9th Cir. 2008). The privacy impact assessment simply provides an analysis of the topics required to be addressed in section 208 of the E-Government Act. That the privacy impact

assessment incorporates certain terms from the Functional Standard, such as the definition of "suspicious activity," or explains (to the extent possible) how the FBI collects, disseminates, and reports terrorist-related activity in eGuardian pursuant to its statutory and regulatory authority, does not suggest that the assessment itself has any separate legal force. The privacy impact assessment instead is consistent with the purpose explained in the OMB Guidance, which is to provide "an *analysis* of how information is handled [in that system] . . . to ensure handling conforms with applicable legal, regulatory, and policy requirements regarding privacy[.]" OMB Guidance, *available at* http: //www.whitehouse.gov/omb/memoranda_m03-22, Attachment A, II.A.f thereto (emphasis added).

For similar reasons, the privacy impact assessment does not trigger the APA's notice-and-comment rulemaking procedures. "Under the APA, a federal administrative agency is required to follow prescribed notice-and-comment procedures before promulgating substantive rules." *Colwell v. Dept. of Health & Human Servs.*, 558 F.3d 1112, 1124 (9th Cir. 2009). As explained, a privacy impact assessment is an "analysis"—not a legislative rule. The privacy impact assessment does not set forth any obligations, or enforcement mechanism, or include any other provision that could be considered substantive obligations.

Indeed, requiring rulemaking for the topics addressed in the privacy impact assessment would be contrary to the procedure set forth by Congress in section 208 of the E-Government Act, which requires the agency to: (1) conduct a privacy impact assessment; (2) ensure review of that privacy impact assessment by the Chief Information Officer, or equivalent; and (3) "if practicable," make the "privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means," Pub. L. No. 107-347, § 208(b)(1)(B)(iii), before "developing or procuring information technology that collects, maintains, or disseminates information that is an identifiable form," *id.* § 208(b)(1)(A)(i), or "initiating a new collection of information" that is an identifiable form, *id.* § 208(b)(1)(A)(ii). There is no basis to contravene the will of Congress in this regard.

C. Plaintiffs' Other Allegations Likewise Fail to Set Forth a Cognizable Claim

Plaintiffs also ask the Court to discern the existence of an allegedly separate, legally binding DOJ standard, Compl. ¶ 69, in certain statements contained in a United States General Accounting Office ("GAO") Report, *id*. ¶ 54, and certain pamphlets, including a "roll call release," Compl. ¶¶ 56-57, but they have failed to allege facts showing that any such standard has been established by these materials or imposed on FSLTT law enforcement partners. *See* Pls. Mem. at 9–12.

The documents cited by Plaintiffs do not articulate any standard for the reporting or sharing of information, but instead simply urge the reporting of counterterrorism, counterintelligence, cyber, and criminal threats to the FBI. As discussed, this broader reporting function is conducted pursuant to the FBI's general investigative authority under 28 U.S.C. § 533 and its general authority to collect records under 28 U.S.C. § 534. *See* Dkt. 51-1, at 9. This reporting function is distinct from the NSI—which involves the sharing of information among FSLTT partners. Indeed, the Functional Standard recognizes the existence of these other information-gathering authorities, *see* Dkt. 51-3, at 17, and explicitly states that "terrorism-related leads that do not meet the requirements of the ISE-SAR Functional Standard but may require investigative follow-up by the FBI . . . may be submitted electronically to the FBI." *Id.* n. 17. Accordingly, while Defendants do not dispute that the FBI encourages the reporting of information even when that information does not satisfy the definition of "suspicious activity" in the Functional Standard, this process is distinct from the NSI, and Plaintiffs have failed to identify any particular information-gathering standard that they are challenging. Without doing so, as discussed, Plaintiffs should not be permitted to take discovery in search of the basis of their DOJ standard claims.

Moreover, even if Plaintiffs had identified the existence of a separate standard in the materials they cite, they have not pled any facts establishing that the FBI has imposed any legal obligation on FSLTT law enforcement partners to report information consistent with that unidentified standard. *Bennett*, 520 U.S. at 177-78; *see also Mamigonian*, 710 F.3d at 942. None of the documents Plaintiffs rely upon plausibly assert the existence of any DOJ or FBI rule

having "'the status of law'" that demands "'immediate compliance'" by FSLTT partners, *Standard Oil Co. of Cal*., 449 U.S. at 239 (internal citation omitted), with regard to reporting or otherwise. Indeed, in describing the pamphlets cited in the Complaint, Plaintiffs correctly identify them to be "guidance," *see* Pls. Mem. at 11. This type of informational guidance cannot be deemed to "command[]" FSLTT partners "to do or forbear from anything." *Fairbanks*, 543 F.3d at 593. Nor would notice-and-comment rulemaking be triggered under these circumstances. Because the broader reporting urged by the FBI does not impose any legal obligations upon FSLTT partners, it cannot be considered a substantive rule that triggers rulemaking. Allowing discovery based on these materials, in support of a purported APA claim, would be without any basis in fact or law.

D. Plaintiffs' Citation of Documents Not Referenced in the Complaint Does Not Entitle Plaintiffs to Discovery

Although not alleged in the Complaint, Plaintiffs also cite to documents not referenced in the Complaint related to the prior existence of two separate systems—eGuardian and Shared Space—for the collection of suspicious activity reports and assert that these two systems applied distinct privacy and retention policies. *See* Pls. Mem. at 12–13. These documents also do not support Plaintiffs' asserted entitlement to discovery.

As an initial matter, this section of Plaintiffs' brief should be disregarded because "[i]t is well-established that parties cannot amend their complaints through briefing or oral advocacy. *S. Walk at Broadlands Homeowner's Ass'n v. Openband at Broadlands*, LLC, 713 F.3d 175, 184 (4th Cir.2013); *see also Bartley v. Wells Fargo Bank*, No. 2:12-CV-02169-GMN, 2014 WL 664660, at *2 n.1 (D. Nev. Feb. 18, 2014) ("Plaintiffs cannot rely on their briefing in opposition to Defendant's motion to amend their inadequate Complaint.").

Even if these assertions were considered and credited at this stage of the litigation, they do not support Plaintiffs' claims of a separate, legally binding "DOJ Standard" or justify discovery. Plaintiffs do not challenge the privacy and retention policies of eGuardian and Shared Space. They challenge the standard by which information is collected, maintained, and shared, and there is nothing in these documents suggesting that these systems adopted different standards in this regard.

III. Even If Plaintiffs' "DOJ Standard" Claim Could Proceed, Discovery Should Not Be Permitted in this APA Action

Even if this Court declines to dismiss Plaintiffs' DOJ Standard claims at this time, discovery should not be permitted at this stage. Instead, Defendants should be permitted to file a motion for summary judgment supported by the already filed administrative record and any additional declarations that are needed to establish that a grant of summary judgment is appropriate. At that time, Plaintiff would be permitted to seek to supplement the record or seek discovery if appropriate. This would narrow the potential issues of dispute and provide a more detailed basis for the Court to determine what, if any, additional information is needed to resolve Plaintiffs' claims.

In an APA case such as this one, "the focal point for judicial review should be the administrative record already in existence, not some new record initially in the reviewing court." *Pitts*, 411 U.S. at 142. And if an administrative record has not been developed setting forth "the reasons for the agency decision," 411 U.S. at 143, that does not permit the development of "some new record made initially in the reviewing court." *Id*. at 142. The appropriate next step would instead be "to obtain from the agency . . . such additional explanation of the reasons for the agency decision as may prove necessary." *Id*. at 143.

Plaintiffs incorrectly assert that Defendants have the burden of demonstrating why discovery should not go forward. Pls. Mem. at 8. To the contrary, the burden is instead on Plaintiffs to show that they are entitled to discovery under one of the narrow exceptions to the well-recognized rule that discovery is not permitted in APA actions. *Bark*, 2 F. Supp. 3d at 1152; *McCrary*, 495 F. Supp. 2d at 1041. Neither *Gray v. First Winthrop Corp*., 133 F.R.D. 39 (N.D. Cal. 1990) nor *Blankenship v. Hearst Corp*., 519 F.2d 418 (9th Cir. 1975), upon which Plaintiffs rely to argue that Defendants bear the burden of showing why discovery should not be allowed, Pls. Mem. at 8, involved an APA action, as here, where discovery is generally not permitted.

The only exception to the rule against discovery that Plaintiffs invoke, Pls. Mem. at 19 n. 17, is where there is a "failure to explain administrative action [so] as to frustrate effective

judicial review.'" *Public Power Council v. Johnson*, 674 F.2d 791, 793 (9th Cir. 1982) (quoting *Pitts*, 411 U.S. at 143). To permit discovery under this exception, the Court (even if the Court were to determine that Plaintiffs' special motion raises issues of material fact) would first have to determine that the matter at issue would not be answered upon the submission of summary judgment briefing on this claim. The exception Plaintiffs rely upon does not provide for the unbounded discovery at this stage. Moreover, "because this exception is so broad in its formulation, courts have been reluctant to invoke it." *Public Power Council*, 674 F.2d at 794. And even when the exception is invoked, "the preferred procedure is remand to the agency for its amplification," "either through affidavits or testimony . . . as may prove to be necessary." *Id.* Discovery is only considered as a last resort, and even at that stage would be strictly "limited," to situations where "serious gaps would frustrate challenges to the agency's action." *Id.*[3]

The other case law relied on by Plaintiffs also fails to establish that they are entitled to discovery. Although Plaintiffs suggest that broad discovery is permitted under *Citizens to Preserve Overton Park, Inc. v. Volpe*, 401 U.S. 402 (1971), Pls. Mem. at at 2, 19-20, *Overton* involved a situation in which the Court was authorized to conduct plenary, *de novo* review. In an action such as this where an action is alleged to be arbitrary and capricious, *de novo* review is not authorized, *Pitts*, 411 U.S. at 142, and the limiting principles of judicial review, and strong presumption against discovery in particular, set forth in *Pitts*, *Public Power Council* and *Asaraco*, apply. Similarly, Plaintiffs' reliance on the Eighth Circuit's decision in *Iowa League of Cities v. EPA*, 711 F.3d 844 (8th Cir. 2013), Pls. Mem. at 23, is misplaced. Plaintiffs, on the basis of that decision, suggest that discovery is appropriate because any administrative record submitted by Defendants is not likely to be complete because Defendants deny that the FBI has issued a distinct rule for the collection, maintenance, and sharing of information that is subject to

[3] Such limited discovery under this exception is in keeping with the Court's role in an APA case like this where an action is alleged to be arbitrary and capricious. In such an action, "[i]f the reviewing court finds it necessary to go outside the administrative record, it should consider evidence relevant to the . . . agency action only for background information . . . or for the limited purposes of ascertaining whether the agency considered all of the relevant factors or fully explicated its course of conduct or grounds of decision." *Asaraco, Inc. v. U.S. Envtl. Prot. Agency*, 616 F.2d 1153, 1160 (9th Cir. 1980).

APA review. Pls. Mem. at 18. But the Eighth Circuit's decision is not binding on this Court, and in any event, that Circuit Court did not recognize a rule different from that set forth in *Pitts*, *Public Power Council*, and *Asaraco*. *See Iowa League of Cities*, 711 F.3d at 864 n.13. Instead, it briefly questioned whether a particular rationale for administrative record review might apply and then denied the motion to supplement the record without deciding that question. *Id*.

In sum, if the Court does not dismiss Plaintiffs' claims at this stage, the correct course would be to deny the pending request for discovery and allow summary judgment briefing to proceed on all claims. Only if Plaintiffs can, in response, establish that their DOJ Standard claims cannot be resolved through normal APA review, would consideration of any discovery then be appropriate.

CONCLUSION

For the foregoing reasons, Plaintiffs' discovery motion should be denied.

July 10, 2015

Respectfully submitted,

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ *Kieran G. Gostin*
PAUL G. FREEBORNE
Senior Trial Counsel
KIERAN G. GOSTIN
Trial Attorney

Civil Division, Federal Programs Branch
U.S. Department of Justice
P.O. Box 883
Washington, D.C. 20044
Telephone: (202) 353-0543
Facsimile: (202) 616-8460
E-mail: paul.freeborne@usdoj.gov

Attorneys for Federal Defendants

CERTIFICATE OF SERVICE

I hereby certify that on July 10, 2015, I filed the above pleading and its attachments with the Court's CM/ECF system, which will send notice of such filing to all parties.

Date: July 10, 2015

/s/ *Kieran G. Gostin*

KIERAN G. GOSTIN